IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF: **ISRAEL FABER** **a/k/a "letit1234" and "Bliz"**	**Case No. 20-1045**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR AN ARREST WARRANT

I, Angela Strause, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since February of 2010. I have investigated federal criminal violations of the United States Code related to drug trafficking, internet crimes against children, human trafficking, fraud, kidnapping and matters related to domestic and international terrorism. In my current assignment, my duties include the investigation of "crimes against children" which includes child exploitation, child pornography, sex trafficking of children and/or adults, and the online sexual exploitation of children. I have received training in the area of investigations of child exploitation and sex trafficking, and have, as part of my daily duties as a Special Agent, investigated violations relating to child pornography, sex trafficking and other crimes pertaining to the exploitation of children such as coercion and enticement, transportation of minors with intent to engage in criminal sexual activity, and travel with intent to engage in illegal sexual activity. As part of my duties as a Special Agent, I have had the opportunity to interview victims and suspects of child exploitation and sex trafficking offenses, observed and reviewed numerous

examples of digital evidence, and participated in the execution of many search warrants involving child exploitation and sex trafficking offenses.

2. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. The statements in this affidavit are based on my personal investigation and information provided by other law enforcement officers. This affidavit is intended to show only that there is sufficient probable cause for the requested arrest warrant and does not set forth all of my knowledge about this matter. The facts and circumstances of this investigation have been summarized for the specific purposes of this application, and for the limited purpose of establishing that probable cause exists for the arrest warrant sought herein.

4. Based on the information set forth in this Affidavit, I respectfully submit there is probable cause to believe that ISRAEL FABER, date of birth 5/25/1987, committed violations of Title 18, United States Code, Section 2251(a) (Manufacture and Attempted Manufacture of Child Pornography).

INVESTIGATION AND PROBABLE CAUSE

A. April 20, 2020 Distribution of Child Pornography by Kik User "Letit1234"

5. On April 20, 2020, at approximately 10:22a.m. EDT, a Task Force Officer ("TFO") with the FBI Washington Field Office ("FBI-WFO"), was acting in an undercover ("UC") capacity as part of the Metropolitan Police Department-Federal Bureau of Investigation ("MPD-FBI") Child Exploitation Task Force, operating out of a satellite office in Washington, D.C. As part of ongoing undercover operations, the UC entered a known private Kik[1] Group in

[1] Your Affiant is aware through training and experience that Kik Messenger (hereinafter "Kik") is a mobile application designed for chatting or messaging owned and operated by Kik Interactive, Inc. According to the

which he previously was a member. The UC was acting as an "administrator" for the Kik Group's owner.[2] This Kik Group is known to the UC as a place where people meet, discuss and trade original images of minor children, links, and videos of child pornography, among other things. The UC had been a member of this particular Kik Group for several weeks.

6. While the UC was in the Kik Group on April 20, 2020, the UC observed a Kik user with the display name "Bliz Banks" and the username "letit1234" enter the Kik Group chat as a new member. According to the UC, as each new member enters the Kik Group chat, a banner appears which describes the rules of the Group. The banner for this Kik Group reads "*Hello! Welcome to the room. You will have to stay active to stay here. Here is what you need to know: Lurkers/inactives will be kicked. Have a profile pic. Don't beg for pics over PM. Ask before you PM. Tell us about yourself when you join. Verify with an admin (pic of you and daughter and a live of you or a live pic of daughter. Easy right"*.

7. Then, acting as an "administrator," the UC informed "letit1234" that he had to verify his identity with the UC in a private chat. In response, "letit1234" contacted the UC in a private chat and identified himself as a 33 year-old dad residing in Delaware. The UC asked "letit1234" to hold up 4 fingers near his daughter's head to verify that he was an actual father

---

publicly available document "Kik's Guide for Law Enforcement," to use this application, a user downloads the application to a mobile phone, computer, or other digital device via a service such as the iOS App Store, Google Play Store, Apple iTunes, or another similar provider. Once the application is downloaded and installed, the user is prompted to create an account and username. The user also creates a display name, which is a name that other users see when transmitting messages back and forth. Once the user has created an account, the user is able to locate other users via a search feature. Kik has a free messenger application which provides cross-platform smartphone instant messaging. Through Kik, users can share text-based conversation, photos, videos and other forms of rich media. Users of Kik can use Kik messenger to engage in multi-user group chats. Kik is available for installation for IOS, Android, Blackberry and Symbian based devices. Kik can be used either with a data plan or through Wi-Fi.

[2] An "owner" of a Kik Group typically is the originator of a particular Group. He or she moderates the Group, sets the rules and designates "administrators," who can act in the owner's place when the owner is unavailable. An "administrator" is often utilized to screen new members and remove members who are not following the rules. Once the group is created, Kik users have the option of sharing a link to the group that includes all of their contacts or any other user. These groups are frequently created with a group name containing a hashtag (#) that is easily identifiable or searchable by keyword.

and that he was communicating in real time. "[L]etit1234" responded, "I'm at work I have pics wit her." Then, "letit1234" sent the UC a gallery picture (which I understand, based on my training and experience, refers to a previously taken—not live—image) of a male wearing a NY Yankees baseball cap and a white T-shirt with his arm around a young female with long dark hair who appears to be in her early teens. The teen is wearing a black and grey sweatshirt with the word "PINK" on it and grey pants. "[L]etit1234" then sent a "live"[3] camera image of himself exposing his face. The UC observed that the male depicted in the "live" camera image matched the male in the gallery picture with the young female teen. "[L]etit1234" then asked the UC for "pics" of his daughter. In response, the UC sent an image of his purported daughter (not a real child).

8. "[L]etit1234" told the UC in the same private chat conversation on April 20, 2020, that he spies on his daughter and has nude images of her. Specifically, the conversation went as follows:

UC:	What kind of pics u have of yours
letit1234:	All kinds I spy
letit1234:	Hbu
…	
letit1234:	I use my phone
letit1234:	Nudes?
…	
UC:	Yeah
UC:	U
letit1234:	Yea

9. Then, "letit1234" sent the UC an image of a young girl exiting a shower which has a white background and a band of colored tile on the upper portion of the shower wall. The image appears to have been taken through the crack of a partially opened door or other

[3] A "live" camera image means that the image was taken in real time, *i.e.*, that the image was taken then immediately sent to the recipient.

obstruction and depicts a young girl with long, dark hair stepping out of the shower. The young girl is fully nude and both breasts and her vagina are exposed. Her right leg is on the floor and her left leg is still in the shower, so her legs are partially spread apart as she is reaching for something that is out of view of the camera. This image was followed by another image from "letit1234" of the same girl exiting the same shower—"letit1234" told the UC: "That's her face," indicating that the girl in the second image is the same girl in the first image. In the second image, the right side of the girl's face can be seen as well as her right breast. Based on my training and experience, I believe the first image constitutes child pornography within the meaning of 18 U.S.C. § 2256, as it depicts the use of a minor in sexually explicit conduct, that is, the lascivious exhibition of the genitals. Based on my training and experience, I believe both images constitute an attempt to manufacture child pornography as well. Both the UC and your Affiant noted that the young girl in these sexually explicit images appears similar to the girl with whom "letit1234" is standing in the original "gallery" photo that was sent to the UC.

10. "[L]etit1234" also sent a third sexually explicit image to the UC of a girl with her back to the camera. Her face is not visible. She is fully nude and her legs are partially spread apart, showing her buttocks. This image also appears to be in the same bathroom as the two images described above in Paragraph 9. Based on my training and experience, I believe that this image also constitutes an attempt to manufacture child pornography.

11. "[L]etit1234" told the UC that he uses his phone to take the pictures and all he currently has are shower pictures of his step-daughter and remarked "until I finish the room."

B. Identification of ISRAEL FABER as Kik User "Letit1234"

12. Based on the content of the UC's chats with Kik user "letit1234," an emergency disclosure request was submitted on April 20, 2020 to Kik c/o MediaLab, requesting subscriber identification information and IP access logs associated with Kik username "letit1234."

13. On April 20, 2020, Kik responded to the request and provided the following subscriber information: a Kik display name of "Bliz Banks," an unconfirmed e-mail address of ONEMORETIME9812@OUTLOOK.COM, a reference to the fact that an iPhone was used as the registration device, and user IP logs spanning March 21, 2020 through April 20, 2020, (including IP addresses and associated port numbers).

14. FBI-WFO examined the IP logs for Kik user "letit1234," and determined that the most frequently accessed IP addresses were: (1) T-Mobile Wireless IP addresses (172.58.191.4, 172.58.188.223, 172.58.203.78, 172.58.190.135, 172.58.206.217), and (2) a Comcast Communications IP address (73.187.65.193).

15. On the same day, April 20, 2020, an emergency disclosure request form was submitted to Comcast Communications requesting subscriber identification and physical service address information associated with IP address 73.187.65.193 Port 63997 on April 17, 2020, at 14:32:14 UTC. Comcast Communications identified the subscriber as "Israel Faber, 117 Honeysuckle Road, Knottingham [*sic*] PA 19362," and provided contact number (610) 606-8825.

16. The Kik IP logs for "letit1234" revealed that T-Mobile Wireless and Comcast IP addresses were used on April 20, 2020, the date of the aforementioned conversations between the UC and "letit1234." Based on my training and experience, I understand that this means that a T-Mobile Wireless mobile device was used to log into and communicate through Kik. The T-

Mobile Wireless IP address accessed via mobile device on April 20, 2020 was 172.58.206.217, which resolved to Philadelphia, Pennsylvania. Comcast IPs 68.33.90.132 and 68.33.90.2 also were accessed on April 20, 2020 and resolved to the Baltimore, Maryland area.[4] During the course of this investigation, I learned that ISRAEL FABER works in Cockeysville, Maryland, which is approximately 17 miles north of Baltimore, Maryland.

17. Upon receipt of this information, FBI-WFO utilized available open source and law enforcement sensitive databases to fully identify the suspected user of Kik account "letit1234" as ISRAEL ALAN FABER, DOB: 05/25/1987, residing at 117 Honeysuckle Road, Nottingham, PA 19362. FABER's criminal history includes convictions beginning in 2006 for multiple counts of simple assault, possession of a controlled substance, criminal mischief, criminal trespass, disorderly conduct and harassment.

18. The UC then compared the "live" camera photo that "letit1234" sent to the UC through Kik and noted that the image matches FABER's Pennsylvania driver's license photo.

19. FBI-WFO also located images of FABER's wife and their children via an open source social networking site. The UC compared photos of the young girl sent by "letit1234" during the Kik chat session with images contained on the social networking site attributed to FABER's wife, and noted that one of the young girls visually matches the minor victim contained in the images sent through Kik. Also, based on FBI-WFO's review of images and other information from FABER's wife's social networking page, there appear to be seven

[4] Later, on May 5, 2020, your Affiant served an administrative subpoena on Comcast Communications requesting subscriber information for these two Comcast IP addresses. Specifically, your Affiant requested subscriber information attributed to IP address 68.33.90.132 using port 28781 at 4:51 a.m. (EDT) and IP 68.33.90.2 using port 7046 at 5:08 a.m. (EDT) on April 20, 2020. On May 7, 2020, responsive records from Comcast identified subscriber information for the two IP addresses as: "Israel Faber, 117 Honeysuckle Road, Nottingham, PA 19362, subscriber phone (610) 606-8825."

children (including the minor victim) living at 117 Honeysuckle Road, all of whom appear to be juveniles.

C. Search of FABER's House on April 22, 2020 and Forensic Review FABER's iPhone

20. On April 21, 2020, the UC re-entered the Kik Group and observed "letit1234" also was in the Group. He noted that "letit1234" complained in a message to the Group that he had shared photos with another user and the user "bounced" on him. He then queried the Kik Group for other fathers willing to trade original (real) images, stating, "Any real dads wanna pm I have real pics and vids."

21. On the next day, April 22, 2020, your Affiant executed a search warrant at the residence located at 117 Honeysuckle Road, Nottingham, Pennsylvania ("117 Honeysuckle Road"), pursuant to Case No. 20-630-M, issued by the Honorable Jacob P. Hart on April 22, 2020. During the search of FABER's residence, a red Apple iPhone 11 was identified as belonging to ISRAEL FABER.

22. FABER was interviewed by your Affiant during the execution of the search warrant at 117 Honeysuckle Road. FABER indicated that his current phone is an iPhone, which was located in the master bedroom. FABER stated that he has always had iPhones in the past, but no longer has any of his old phones. FABER told your Affiant that he trades in his old phones to T-Mobile (his service provider) in order to receive credit toward a new phone. FABER was informed that his iPhone 11 would be searched and he advised your Affiant there is no passcode on this device. During his interview, FABER admitted to your Affiant and an FBI TFO that FABER has heard of Kik and described it as an application people use to chat, but he denied ever using the Kik app or ever having a Kik account. FABER denied ever taking any sexually explicit photos of his step-daughter.

23. During the search of 117 Honeysuckle Road, your Affiant examined the master bathroom, which is accessed by passing through the master bedroom shared by FABER and his wife. Your Affiant compared the shower layout and noted the distinct frosted glass sliding door as well as the band of colored tile located at the top portion of the shower and confirmed that it is the same shower in the sexually explicit images of the minor girl victim identified in Paragraph 9, above. Your Affiant learned from speaking with FABER's wife that, despite the fact that the residence contains a second full bathroom, all seven minor children living at the residence regularly use this master bathroom.

24. An on-site preliminary review of FABER's seized iPhone 11 yielded multiple images, including the image identified in Paragraph 7, as having been sent to the UC by "letit1234" on April 20, 2020 which depicted FABER wearing a NY Yankees baseball cap and a white T-shirt with his arm around a young female with long dark hair who appears to be in her early teens. The teen is wearing a black and grey sweatshirt with the word "PINK" on it and grey pants. Your Affiant reviewed this image and noted that the same minor female is also depicted in the sexually explicit images described in Paragraph 9. However, the image found on FABER's phone as described in this paragraph (and Paragraph 7) appears to be an older image because the minor female looks younger in this image than in the sexually explicit images. The on-site, preliminary review of FABER's cellular device did not yield images or videos depicting child pornography.

25. There is evidence that FABER has, in fact, used the Kik app, including on April 20, 2020, despite his denials to your Affiant and other law enforcement agents on April 22, 2020. A forensic examiner, who is currently a TFO with the FBI's Capital City Child Exploitation Task Force, conducted a deeper analysis of the forensic material located on FABER's iPhone. The

forensic examiner was able to confirm, through analysis of the iPhone's Application Usage log, that the Kik application had been "installed" and "un-installed" on FABER's iPhone almost daily, and sometimes multiple times per day, since at least April 1, 2020. Examination of the Network Data Usage Database specifically confirmed that FABER's iPhone accessed the Kik application on April 20, 2020, the date of the Kik chat communications between the UC and Kik user "letit1234," as described above in this Affidavit. The last recorded "installation" of the Kik app on FABER's iPhone occurred on April 21, 2020 at 6:23 a.m. and the last recorded "un-installation" of the Kik app on FABER's iPhone occurred on April 21, 2020 at 2:21 p.m. Based on my training and experience, your Affiant knows that Kik users wishing to conceal the content of their Kik communications often un-install and re-install the Kik app in order to remove all content associated with the chat sessions occurring during each period of installation. According to Kik's Law Enforcement Guide, which was last revised on February 26, 2020, "the text of chat messages **are stored locally on the Kik user's device.** [Kik does] not see, store, or have access to chat message conversations in [their] systems." (Emphasis in original.) Thus, your Affiant is aware that by continuing to un-install and re-install the Kik app, a user can essentially wipe clean all prior chat sessions because the content is stored only on the user's device and is not maintained on Kik's servers.

26. In further reviewing the contents of FABER's iPhone, the forensic examiner also accessed saved Portable Document Format (.pdf)[5] files and identified five (5) sexually explicit images depicting young minor female children in the same bathroom described above in

[5] Your Affiant knows that .pdf files are typically identified with Adobe Acrobat software. According to Adobe Systems, documents from any application can be converted to a .pdf file, however, through training and experience, Your Affiant knows this is an unusual file format to use for image files. The most commonly used formats for images are .tiff, .jpeg, .png and .gif.

Paragraphs 9 and 10, which was positively identified by Your Affiant as the master bathroom observed during the search of 117 Honeysuckle Road (FABER's house) on April 22, 2020. Your Affiant reviewed each image, and the forensic examiner identified the corresponding file name and associated file path for each image. These images depict three identified girl victims, including one victim who was around 5 years old at the time. One of the .pdf images depicts two child victims, including the 5-year old victim, who is shown bending over with her anus and vagina exposed to the camera. Your Affiant believes that this image, as well as several others found in .pdf form on FABER's iPhone, constitute child pornography within the meaning of 18 U.S.C. § 2256.

27. Information from FABER's iPhone provided additional evidence that "Bliz" was a nickname used by FABER. One of the five sexually explicit .pdf images found FABER's iPhone had the file name "Mail – Bliz Bang – Outlook.pdf". Furthermore, a TextMe[6] account was located in FABER's iPhone with the username "BLIZ367956". This information—in addition to evidence that "Bliz Banks" was FABER's Kik display name (*see* Paragraphs 12-19) and that an Outlook e-mail address associated with FABER contained "Bliz" (*see* Paragraph 30, below)—further corroborates that "Bliz" is a nickname used by FABER.

28. Information from FABER's iPhone also revealed that FABER likely used Outlook when viewing, accessing, or otherwise possessing child pornography. Your Affiant noted that the .pdf image described above refers to Outlook in its filename: "Mail – Bliz Bang – **Outlook**.pdf" (emphasis added). This reference suggests that this sexually explicit .pdf image

[6] Your Affiant understands that TextMe is a free application offering free unlimited texts, calling and picture messaging to any phone in U.S., Canada and 40 countries in the world. The App allows users to send pictures, voice and video messages to other users and transforms an iPod, iPad or tablet into a "real" phone. The App also allows users to send Dropbox photos and videos via SMS directly from TextMe.

(or the original source image or video) was stored on, was transferred using or otherwise involved Outlook. Also, in reviewing the sexually explicit images previously described in Paragraph 26, your Affiant noted that at least two of the images appeared to be screenshots taken from a site accessed through the internet. Located at the top of the image in what would be the "address bar" portion was the phrase "outlook.live.com."

29. Forensic analysis of FABER's iPhone App libraries revealed that FABER had been backing up his phone content to several cloud storage accounts, including Microsoft OneDrive.

D. Additional Evidence in Electronically Stored Data

30. The investigation, to date, has revealed that FABER has at least two Outlook e-mail addresses associated with him. In addition to the e-mail address ONEMORETIME9812@OUTLOOK.COM, which was used to create the Kik account "letit1234" from which child pornography was distributed, forensic analysis revealed that FABER also is associated with e-mail address BLIZ36@OUTLOOK.COM.

31. On May 6, 2020, your Affiant served on Microsoft Corporation search warrant 20-720, issued by the Honorable Thomas J. Rueter on May 5, 2020. On May 18, 2020, responsive records were received from Microsoft providing content for e-mail accounts BLIZ36@OUTLOOK.COM and ONEMORETIME9812@OUTLOOK.COM.[7]

32. Your Affiant reviewed the responsive e-mail data related to the BLIZ36@OUTLOOK.COM account, and noted that the account was registered on December 8,

[7] The search warrant also requested content for an OneDrive account associated with Israel36Faber@gmail.com. Microsoft could not locate data for the OneDrive account associated with that e-mail account, with the exception of a Registration Profile titled "Israel36Faber@Gmail.com; Izzy Faber".

2017 to "Bliz Bang". The account ONEMORETIME9812@OUTLOOK.COM was registered to "Bliz Banks" on September 20, 2019 at 10:07 a.m. Only moments later, this account was used to create Kik account "letit1234", as your Affiant noted a "Welcome to Kik" e-mail from "NO-REPLY@KIK.COM" to ONEMORETIME9812@OUTLOOK.COM dated September 20, 2019 at 10:10 a.m., verifying a Kik account set-up for username "letit1234".

33. The BLIZ36@OUTLOOK.COM e-mail account also included an e-mail dated August 9, 2019 at 18:19 (UTC), in which a OneDrive link (*i.e.*, a hyperlink that, if clicked, would connect to content in the OneDrive account) was sent fromBLIZ36@OUTLOOK.COM to BLIZ36@OUTLOOK.COM. The link connects to a video, which is 00:01:19 (one minute, nineteen seconds) in duration and contains an identified juvenile female in the master bathroom of 117 Honeysuckle Road. The camera is pointed toward the bathroom mirror and captures the juvenile female, who has just emerged from the shower. She can be seen bending over and wrapping her hair in a multi-colored striped towel. The camera then captures the juvenile's left breast as she turns and bends over, also briefly exposing her anus as she puts on her underwear and bra. A male voice can be heard yelling from the outside of the bathroom asking the juvenile if she's done yet. The juvenile finishes getting dressed in shorts and a t-shirt,[8] gathers up her clothing and begins to exit the bathroom. As she is walking out, an adult male, wearing dark-colored shorts, a white t-shirt and a white baseball cap (worn backwards), positively identified as ISRAEL FABER, immediately enters the bathroom. FABER turns to close the door behind the juvenile as she exits. FABER then immediately bends down and reaches for the camera. At this point in the video, FABER's face and arm tattoos are clearly visible, just prior to him turning off

[8] Your Affiant believes, based on the child victim's clothing and other information learned in this investigation, that this video was likely produced in a warmer month of 2019.

the camera. This video is evidence of a violation of 18 U.S.C. § 2251(a), Manufacturing and Attempted Manufacturing of Child Pornography, and is the basis of the Count as described in Attachment A to this Affidavit.

34. Your Affiant reviewed e-mail content for the BLIZ36@OUTLOOK.COM account and noted at least nine (9) separate instances during which FABER e-mailed images to himself—specifically, these e-mails were sent from the BLIZ36@OUTLOOK.COM account to the BLIZ36@OUTLOOK.COM account between the time period August 23, 2019 to September 1, 2019.[9] Contained within those emails were 21 attachments of images depicting child exploitative and/or child pornography material. A review of the images resulted in the positive identification of three minor girl victims (the same three minor girl victims identified in the .pdf files on FABER's iPhone, *see* Paragraph 26), and all of the images were taken in the same master bathroom as the images described in Paragraphs 9 and 10, which is the same master bathroom positively identified by Your Affiant during the search of 117 Honeysuckle Road, as referenced in Paragraph 23. At least three (3) of the image attachments were identical to those sent to the UC on April 20, 2020, as referenced in Paragraphs 9 and 10. At least five (5) of the image attachments were identical to the .pdf file images located on FABER's iPhone, as referenced in Paragraph 26.

[9] Through training and experience, as well as information learned from other law enforcement officers, one reason users choose to "transfer" images to and from the same account is for ease in saving the images to different devices without having to physically "connect" one device to another. Another reason users may email images within the same account is to minimize the risk of detection, which sometimes occurs when images are uploaded or downloaded directly to an application or social media service.

CONCLUSION

35. Based on the forgoing, I submit that this affidavit supports probable cause to believe that ISRAEL ALAN FABER committed violations of Title 18, United States Code, Section 2251(a) (Manufacture and Attempted Manufacture of Child Pornography). Therefore, I request that the Court issue the proposed arrest warrant.

REQUEST FOR SEALING

36. This Court should issue an Order that the arrest warrant, affidavit and application, and all accompanying documents, be filed under seal. Disclosure of this information would compromise this ongoing investigation by alerting the subjects of this investigation and likely causing them to flee and/or destroy evidence. Accordingly, I respectfully request that the arrest warrant specified above be issued and that the same be filed under seal.

Respectfully submitted,

/s/ Angela Strause

Angela Strause
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to
before me on June 19, 2020.

/s/ Marilyn Heffley

HONORABLE MARILYN HEFFLEY
UNITED STATES MAGISTRATE JUDGE